PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-059604
(43)Date of publication of application : 25.02.2000

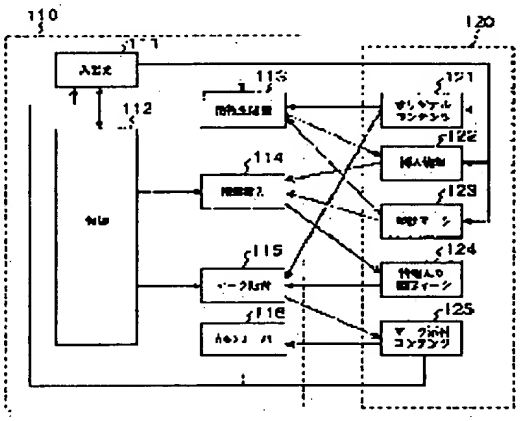
(51)Int.Cl. H04N 1/387
G06T 1/00
G09C 5/00

(21)Application number : 10-226882
(22)Date of filing : 11.08.1998

(71)Applicant : HITACHI LTD
(72)Inventor : YOSHIURA YUTAKA
SUZAKI SEIICHI
NAGAI YASUHIKO
SHINODA TAKASHI

(54) METHOD FOR ATTACHING INFORMATION TO IMAGE AND METHOD FOR EXTRACTING INFORMATION FROM IMAGE

(57)Abstract:
PROBLEM TO BE SOLVED: To attach information to image data while keeping the visibility of images indicated by the image data to a certain degree.
SOLUTION: An information insertion part 114 changes the image size of a graphic mark 123 so as to turn the number of vertical and horizontal pixels to 32 × n+a respectively. In this case, (a) is a decimal number indicated by the bit string of 5 bits of insertion information 122 to be buried and (n) is a numerical value for making 32 × n+a closest to the original image size (128, in this case) of the graphic mark 123. Also, the respective pixel values of the graphic mark 123 are changed so as to make the average value/contrast of the pixel values of the entire graphic mark 123 to 32 × n+a. In this case, (a) is the decimal number indicated by the bit string of 5 bits to be buried and (n) is the numerical value for making 32 × n+a closest to the average value/ contrast of the original pixel values of the entire graphic mark 123.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－59604
（P2000－59604A）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｎ　1/387		Ｈ０４Ｎ　1/387		５Ｂ０５７
Ｇ０６Ｔ　1/00		Ｇ０９Ｃ　5/00		５Ｃ０７６
Ｇ０９Ｃ　5/00		Ｇ０６Ｆ　15/66	Ｂ	

審査請求　未請求　請求項の数19　ＯＬ　（全 13 頁）

(21)出願番号　特願平10－226882

(22)出願日　平成10年８月11日(1998.8.11)

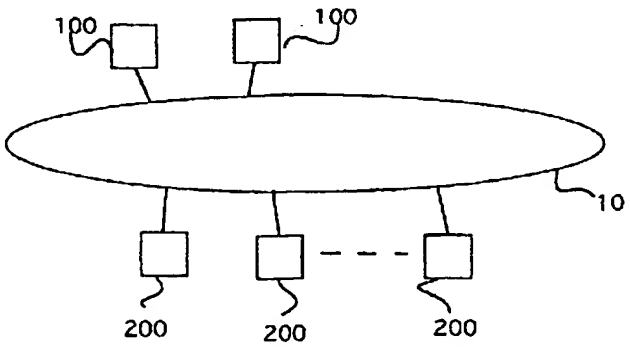
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　吉浦　裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　画像への情報添付方法および画像からの情報抽出方法

(57)【要約】
【課題】イメージデータが表す画像の視認性をある程度保ちながら、イメージデータに情報を添付する。
【解決手段】情報挿入部１１４は、図形マーク１２３の画像サイズを、縦横それぞれの画素数が、３２×ｎ＋ａになるように変更する。ここで、ａは、埋め込む挿入叙法１２２の５ビットのビット列が表す１０進数であり、ｎは、３２×ｎ＋ａを、最も図形マーク１２３の元の画像サイズ（この場合は１２８）に近くする数値である。また、図形マーク１２３の各画素値を、その図形マーク１２３の全体の画素値の平均値／コントラストが３２×ｎ＋ａになるように変更する。ここで、ａは、埋め込む５ビットのビット列が表す１０進数であり、ｎは、３２×ｎ＋ａを、図形マーク１２３全体の元の画素値の平均値／コントラストに最も近くする数値である。

図１



【特許請求の範囲】
【請求項１】画像情報に非画像情報を添付する、画像への情報添付方法であって、
画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、
前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を有することを特徴とする画像への情報添付方法。
【請求項２】請求項１記載の画像への情報添付方法であって、
前記画像の特徴値は、当該画像のサイズであることを特徴とする画像への情報添付方法。
【請求項３】請求項１記載の画像への情報添付方法であって、
前記画像の特徴値は、当該画像全体の輝度値もしくは色値の平均値であることを特徴とする画像への情報添付方法。
【請求項４】請求項１記載の画像への情報添付方法であって、
前記画像の特徴値は、当該画像全体の輝度値もしくは色値のコントラスト値であることを特徴とする画像への情報添付方法。
【請求項５】画像情報に非画像情報を添付する、画像への情報添付方法であって、
画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、
前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、
前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を有することを特徴とする画像への情報添付方法。
【請求項６】画像情報に非画像情報を添付する、画像への情報添付方法であって、
画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、
前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、
前記画像情報に、前記生成した他の画像情報を添付するステップと、を有することを特徴とする画像への情報添付方法。
【請求項７】請求項１、２、３、４、５または６記載の画像への情報添付方法であって、
前記非画像情報として、前記画像情報に関連する所定の情報を、所定の前記画像情報の関係者の公開鍵暗号技術に従った秘密鍵で暗号化した電子署名を生成するステップを、さらに有することを特徴とする画像への情報添付方法。
【請求項８】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、
画像情報を入力するステップと、
前記入力した画像情報が表す画像の特徴値を求めるステップと、
前記求めた画像の特徴値と所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。
【請求項９】請求項８記載の画像からの情報抽出方法であって、
前記画像の特徴値は、当該画像のサイズであることを特徴とする画像からの情報抽出方法。
【請求項１０】請求項８記載の画像からの情報抽出方法であって、
前記画像の特徴値は、当該画像全体の輝度値もしくは色値の平均値であることを特徴とする画像からの情報抽出方法。
【請求項１１】請求項８記載の画像からの情報抽出方法であって、
前記画像の特徴値は、当該画像全体の輝度値もしくは色値のコントラスト値であることを特徴とする画像からの情報抽出方法。
【請求項１２】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、
画像情報を入力するステップと、
前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、
前記入力した画像情報から、前記判別した領域に含まれる画像パターンを抽出するステップと、
前記抽出した画像パターンと所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。
【請求項１３】非画像情報が添付された画像情報から当該非画像情報を抽出する、画像からの情報抽出方法であって、
画像情報と当該画像情報に添付された他の画像情報とを入力するステップと、
前記入力した他の画像情報と所定の規則とに応じて定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を有することを特徴とする画像からの情報抽出方法。
【請求項１４】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報と当該画像情報に添付すべき非画像情報とを入

力するステップと、
前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【請求項１５】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、
前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、
前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【請求項１６】画像情報に非画像情報を添付するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、
前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、
前記画像情報に、前記生成した他の画像情報を添付するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【請求項１７】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報を入力するステップと、
前記入力した画像情報が表す画像の特徴値を求めるステップと、
前記求めた画像の特徴値と所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【請求項１８】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報を入力するステップと、
前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、
前記入力した画像情報から、前記判別した領域に含まれる画像パターンを抽出するステップと、
前記抽出した画像パターンと所定の規則とに従って定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【請求項１９】非画像情報が添付された画像情報から当該非画像情報を抽出するためのプログラムが記録された記録媒体であって、
当該プログラムは、情報処理装置に、
画像情報と当該画像情報に添付された他の画像情報とを入力するステップと、
前記入力した他の画像情報と所定の規則とに応じて定まる値を、前記入力した画像情報に添付された非画像情報として抽出するステップと、を実行させることを特徴とするプログラムが記録された記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、イメージデータが表す画像の視認性を保ちながら、当該イメージデータに他のデータを添付する技術に関するものである。
【０００２】
【従来の技術】イメージデータが表す画像視認性を保ちながら、当該イメージデータに他のデータを添付する技術としては、電子透かし（digital watermark）と呼ばれる技術が知られている。
【０００３】この技術は、IBM SYSTEMS JOUNAL, VOL 35, NOS 3&4, 1996の313頁から336頁のTechniquesfor data hiding などに記載されているように、イメージデータの著作権などの管理情報を、イメージデータ自体にイメージデータと不可分に埋め込む技術である。
【０００４】この電子透かしの技術は、次のような特徴を持っている。すなわち、埋め込まれた情報は、情報を埋め込んだイメージデータが表す画像を表示した場合にも、一般的には視認されず、また、視認可能な範囲において、画像自体をほとんど変化させない。一方、埋め込まれた情報のみを正確に除去することは容易でない反面、不正確に除去すると画像の画質が著しく劣化する。また、一般的には、ある程度までは、イメージデータを圧縮した場合にも、埋め込んだ情報を復元することができる。
【０００５】一方、従来より、インターネットのようなオープンなネットワークを利用する、WWW（World Wide Ｗｅｂ）サーバプログラムとブラウザプログラムとを用いるWWWシステムが知られている。
【０００６】ここで、WWWシステムは、情報を公開するためのWWWサーバプログラムが動作する少なくとも一つのWWWサーバと、当該公開情報を閲覧するためのブラウザプログラムが動作する少なくとも一つのクライアント端末と、からなるシステムである。WWWサーバとクライアント端末との間で、ＨＴＴＰ（Hyper TextTransfer Protocol）と呼ばれる通信プロトコルにより、データのやり取りを行う。

【０００７】WWWサーバで情報を公開する場合、まず、当該サーバに格納された公開すべきテキストデータ、イメージデータ、オーディオデータ、ビデオデータ、あるいは、他のＷｅｂページへのハイパーリンクデータなどを、ＨＴＭＬ（Hyper TextMakeup Language）と呼ばれる構造記述言語を用いて、相互に関連付けて一纏めにしたＷｅｂページを作成する。次に、このＷｅｂページを、他のコンピュータ（クライアント端末や他のWWWサーバ）からアクセス可能な状態で、WWWサーバの任意の格納場所（ディレクトリ）に保管する。

【０００８】一方、公開されたＷｅｂページを、ユーザがクライアント端末からブラウザプログラムを用いて閲覧する場合、クライアント端末を利用するユーザがブラウザプログラムに対して、上記ＷｅｂページのＵＲＬ（Universal Resource Locator）を指定すると、そのＷｅｂページのデータが、WWWサーバよりクライアント端末に送られる。そして、そのＷｅｂページに含まれるテキストデータ、イメージデータ、ビデオデータなどがクライアント端末の画面上に表示される。また、オーディオデータが、当該クライアント端末に接続されたスピーカーなどから出力される。

【０００９】ところで、近年では、このようなWWWシステムをビジネスに利用しようという動きが顕著である。たとえば、WWWシステムにより商品情報を公開するいわゆる電子商取引システムなどは、そのようなビジネス利用の代表例である。

【００１０】このような電子商取引システムでは、販売者は、自己のＷｅｂページに利用可能なクレジットカード会社のロゴマークなどのイメージデータを含め、消費者が支払方法を一目で認識できるようにすることが多い。これは、現実世界（インターネットのような仮想な世界ではない）において、各販売店（クレジットカード会社の加盟店）に、そこで使用可能なクレジットカードのロゴマークを掲示するのに相当する。

【００１１】また、この他、Ｗｅｂページの発信者を示すロゴマークや、そのＷｅｂページを承認した何らかの権限ある個人／機関を示すロゴマークなどのイメージデータを、Ｗｅｂページに含め、Ｗｅｂページの利用者が、一目で、Ｗｅｂページの発信者やＷｅｂページが権限ある個人／機関に承認されていることを認識できるようにすることもある。

【００１２】また、従来、電子データと個人／機関との関係を認証可能とする技術として、電子署名と呼ばれる技術が知られている。

【００１３】電子署名は、電子データの真正さを保証するための技術であり、公開鍵暗号技術と一方向性関数を組み合わせたものである。

【００１４】この技術では、まず、ｇ（ｆ（ｎ，Ｓ），Ｖ）＝ｎと、ｆ（ｇ（ｎ，Ｖ），Ｓ）＝ｎとが成立する秘密鍵Ｓ、公開鍵Ｖの組を作成する。ここで、ｎは任意のデータ、ｆ、ｇは所定の関数であり、上記式は、秘密鍵Ｓを用いて暗号化した任意のデータは公開鍵Ｖを用いて復号化することができ、また、逆に、公開鍵Ｖを用いて暗号化した任意のデータは秘密鍵Ｓで復号化できることを表している。また、ここで、公開鍵Ｖから秘密鍵Ｓを求めることは実質的に不可能となっている。

【００１５】秘密鍵Ｓ、公開鍵Ｖを作成したならば、作成者は公開鍵Ｖを、相手方に渡し、秘密鍵Ｓは作成者が秘密に保持する。

【００１６】そして、鍵の作成者が、相手方にデータを送る場合には、データを所定の一方向関数で評価した評価値を秘密鍵Ｓで暗号化した電子署名を、データに添付して相手方に渡す。

【００１７】ここで、一方向関数は、実質上、データから関数で評価した評価値を算出可能であるが、評価値から元のデータを算出することは実質的に不可能である性質をもつ。また、この電子署名で用いる一方向関数には、実質的に異なるデータに対して異なるビット列を返す関数であること、すなわち、異なるデータに対して同じビット列を返す確率が極めて低い関数であること必要となる。このような関数としては、データの評価値として所定のビット列を返す一方向ハッシュ関数などが知られている。ここで一方向ハッシュ関数をｈで表した場合の、データＤの一方向ハッシュ関数による評価値ｈ（Ｄ）をＤのハッシュ値と呼ぶ。

【００１８】さて、電子署名が添付されたデータを受け取った相手方は、データを一方向関数で評価して評価値を求め、この評価値が、電子署名を公開鍵Ｖを用いて復号化した値と一致するかを検証する。そして、一致した場合には、電子署名が公開鍵Ｖに対応する秘密鍵Ｓの保持者によって成されたものであり、かつ、その電子署名の対象が受け取ったデータであることを認証する。

【００１９】

【発明が解決しようとする課題】前記電子透かしの技術によれば、イメージデータの画像サイズに、イメージデータが表す画像の視認性を保ちながら埋め込める情報量が依存するため、画像サイズの小さなイメージデータに多くの情報を埋め込むことができないという問題がある。

【００２０】このため、たとえば、前述したＷｅｂページ上のロゴマークのような小さな画像サイズのイメージデータには、わずかの情報しか埋め込むことができない。

【００２１】一方、Ｗｅｂページ上にロゴマークをイメージデータとして含める技術によれば、ロゴマークが単なるイメージデータであるため、ロゴマークが示す個人／機関との関係をＷｅｂページが真に有しているのかどうかを認証することができないという問題がある。

【００２２】このため、たとえば、前記クレジット会社のロゴマークを例にとれば、不正者が、当該クレジット

カード会社の正規加盟店のＷｅｂページから当該ロゴマークをコピーし、自己の販売店のＷｅｂページの適当な個所に該ロゴマークを貼り付けてから、該Ｗｅｂページを他のコンピュータからアクセス可能な状態で、WWWサーバの任意の格納場所に保管した場合、消費者は、不正者のＷｅｂページに含まれる上記クレジットカード会社のロゴマークを見て、その不正者が正規の加盟店であるものと判断し、自己のクレジットカード番号など決済に必要なデータを当該WWWサーバに送信してしまう可能性がある。結果、不正者は、入手した消費者のクレジット番号を不正に入手し不正な利益を得ることが可能となる。

【００２３】そこで、本発明は、イメージデータが表す画像の視認性をある程度保ちながら、イメージデータに情報を添付する新たな手法を提供することを課題とする。

【００２４】また、本発明は、Ｗｅｂページ上のロゴマークなどの小さい画像サイズのイメージデータにイメージデータが表す画像の視認性をある程度保ちながら添付した情報によって、そのイメージデータに関連する事項の真正さを認証可能とすることを課題とする。

【００２５】

【課題を解決するための手段】前記課題達成のために、本発明は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した画像情報を、当該画像情報が表す画像の特徴値が、前記入力した非画像情報の値と所定の規則とに応じて定まる値となるように変更するステップと、を有することを特徴とする。

【００２６】ここで、画像の特徴値としては、たとえば、当該画像のサイズや、当該画像全体の輝度値もしくは色値の平均値、あるいは、当該画像全体の輝度値もしくは色値のコントラスト値などの統計的特徴値などが考えられる。

【００２７】本発明では、画像の特徴値の変更によって非画像情報を画像情報へ添付する。このような方法によれば、画像の特徴値の変更の度合いが、画像情報が表す画像の視認性がある程度確保できるレベル以下となるようにすることにより、画像情報が表す画像の視認性も確保しながら、非画像情報を画像情報へ添付することが可能となる。

【００２８】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報が表す画像の特徴値を求め、前記求めた画像の特徴値と所定の規則とに従って定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【００２９】また、本発明の他の態様は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した画像情報の表す画像中において、背景をなす領域を判別するステップと、前記入力した画像情報を、前記判別した背景をなす領域の画像パターンが、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンとなるように変更するステップと、を有することを特徴とする。

【００３０】この態様では、画像の背景領域の画像パターンの変更によって非画像情報を画像情報へ添付する。このような方法によれば、画像の背景領域における画像パターンの変更の度合いが、画像情報が表す画像の視認性がある程度確保できるレベル以下となるようにすることにより、画像情報が表す画像の視認性も確保しながら、非画像情報を画像情報へ添付することが可能となる。

【００３１】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報が表す画像中において背景をなす領域を判別し、判別した領域に含まれる画像パターンを当該画像情報が表す画像から抽出し、そして、抽出した画像パターンと所定の規則とに従って定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【００３２】また、本発明のさらに他の態様は、画像情報に非画像情報を添付する、画像への情報添付方法であって、画像情報と当該画像情報に添付すべき非画像情報とを入力するステップと、前記入力した非画像情報の値と所定の規則とに応じて定まる画像パターンを含む画像を表す他の画像情報を生成するステップと、前記画像情報に、前記生成した他の画像情報を添付するステップと、を有することを特徴とする。

【００３３】この態様では、画像情報に、非画像情報により特定される画像パターンを有する他の画像情報を添付することにより、非画像情報を画像情報へ添付する。このような方法によれば、非画像情報の添付対象である画像情報が表す画像の視認性に影響を与えることなく、非画像情報を画像情報へ添付することが可能となる。

【００３４】なお、このようにして添付された非画像情報を画像情報から抽出するには、当該画像情報に添付された他の画像情報と所定の規則とに応じて定まる値を、当該画像情報に添付された非画像情報として抽出すればよい。

【００３５】なお、上記の各態様において、画像情報に添付すべき非画像情報として、当該画像情報に関連する所定の情報を、当該画像情報の関係者の公開鍵暗号法に従った秘密鍵で暗号化した電子署名を用いれば、画像情報と、当該画像情報に関連する所定の情報と、当該画像情報の関係者との関係の真正さを認証可能とすることができる。

【００３６】

【発明の実施の形態】以下、本発明の実施形態を、WWWシステムにおいてＷｅｂページに貼り付けるロゴマー

クなどの図形マークに情報を埋め込む場合への適用を例にとり説明する。

【００３７】まず、第１の実施形態について説明する。

【００３８】図１に、本第１実施形態に係るWWWシステムの構成を示す。

【００３９】図示するように、本第１実施形態に係るWWWシステムは、Ｗｅｂページであるコンテンツを配布するサーバ側装置１００と、Ｗｅｂページをブラウズする通常複数のクライアント側装置２００より構成される。

【００４０】サーバ側装置１００とクライアント側装置２００の間のＷｅｂページや、その他の情報のやりとりは、ネットワーク１０を介して行われる。

【００４１】図２に、サーバ側装置１００の構成を示す。

【００４２】図示するように、サーバ側装置１００は、処理部１１０と記憶部１２０よりなる。また、処理部１１０は、各種入出力を担う入出力部１１１、サーバ側装置１００内の各部の制御を行う制御部１１２、認証用の情報などの図形マークに埋め込む情報である挿入情報１２２を生成する情報生成部１１３、図形マークに情報を埋め込む情報挿入部１１４、情報を埋め込んだ図形マークをＷｅｂページに貼り付けるマーク貼付部１１５、および、Ｗｅｂページをネットワーク上に公開するＷｅｂサーバ部１１６よりなる。また、記憶部１２０は、図形マーク１２２を貼り付ける前のＷｅｂページであるオリジナルコンテンツ１２１、図形マークに埋め込む情報である挿入情報１２２、情報を埋め込む図形マーク１２３、情報を埋め込んだ図形マーク１２４、および、情報を埋め込んだ図形マークを貼付たＷｅｂページであるマーク添付コンテンツ１２５を記憶する。Ｗｅｂサーバ部１１６は、このマーク添付コンテンツ１２５をネットワーク１０上に公開する。

【００４３】次に、図３にクライアント側装置２００の構成を示す。

【００４４】図示するように、クライアント側装置２００は、処理部２１０と記憶部２２０よりなる。また、処理部２１０は、各種入出力を担う入出力部２１１、クライアント側装置２００内の各部の制御を行う制御部２１２、および、ネットワーク上のＷｅｂサーバよりＷｅｂページを取り込み出力するブラウザ部２１３を備えている。また、処理部２１０は、ブラウザ部２１３が取り込んだＷｅｂページが、マーク添付コンテンツ２２１である場合に、マーク添付コンテンツ２２１から情報入り図形マーク２２２を切り出す情報入りマーク切り出し部２１４、情報入り図形マーク２２２から挿入情報２２３を抽出する情報抽出部２１５、および、挿入情報２２３を用いて認証処理を行う認証部２１６を備えている。

【００４５】記憶部２２０は、マーク添付コンテンツ２２１、情報入り図形マーク２２２、挿入情報２２３、認証処理に用いる公開鍵情報２２４、図形マーク２２５などを記憶している。

【００４６】ここで、サーバ側装置１００やクライアント側装置２００は、図４に示すように、ＣＰＵ３０１や、主記憶３０２、ハードディスク装置である外部記憶装置３０３ｂ、他の外部記憶装置である３０３ａ、通信制御装置３０４、キーボードやポインティングデバイスなどの入力装置３０５、表示装置などの出力装置３０６などを備えた、一般的な構成を有する電子計算機上に構築することができる。

【００４７】この場合、サーバ側装置１００の処理部１１０、および、処理部１１０の内部の各部は、ＣＰＵ３０１が主記憶３０２にロードされたプログラムを、適当なOS上で実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶３０２や外部記憶装置３０３ａ、ｂが、サーバ側装置１００の記憶部１２０として使用される。また、同様に、クライアント側装置２００の処理部２１０、および、処理部２１０の内部の各部は、ＣＰＵ３０１が主記憶３０２にロードされたプログラムを実行することにより電子計算機上に具現化されるプロセスとして実現される。また、この場合、主記憶３０２や外部記憶装置３０３が、クライアント側装置２００の記憶部２２０として使用される。

【００４８】前述した主記憶３０２にロードされＣＰＵ３０１によって実行されることにより、電子計算機上にサーバ側装置１００とクライアント側装置２００を構成するためのプログラムは、予め、外部記憶装置３０３ｂに記憶され、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。または、可搬型の記憶媒体３０７、たとえば、ＣＤ－ＲＯＭを扱う外部記憶装置３０３ａを介して、直接、必要に応じて、可搬型の記憶媒体３０７から主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。もしくは、一旦、可搬型の記憶媒体を扱う外部記憶装置３０３ａを介して、可搬型の記憶媒体３０７から、ハードディスク装置などの外部記憶装置３０３ｂ上にインストールされた後、必要に応じて主記憶３０２にロードされ、ＣＰＵ３０１によって実行される。

【００４９】以下、サーバ側装置１００とクライアント側装置２００の行う処理の詳細を説明する。

【００５０】まず、サーバ側装置１００の行う処理について説明する。

【００５１】制御部１１２は、入出力部１１１とから、オリジナルコンテンツ１２１と、オリジナルコンテンツ１２１に貼り付ける図形マーク１２３を受け入れ、一旦、記憶部１２０に記憶する。一方、情報生成部１１３は、図形マークに埋め込む挿入情報１２３を生成し、記憶部１２０に記憶する。

【００５２】ここで、情報生成部１１３は、図形マーク

に埋め込む挿入情報１２３として、図形マークによって認証可能とする事項を認証するために必要な情報を生成する。たとえば、図形マークがロゴマークであり、そのロゴマークの真正さを認証可能とするのであれば、情報生成部１１３は、図形マーク１２３のハッシュ値を、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報１２３として生成する。この秘密鍵は、あらかじめ記憶部１２０に記憶しておき、これを情報生成部１１３が読み込むようにする。

【００５３】また、たとえば、図形マークがロゴマークであり、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ１２１との関係の真正さを認証可能とするのであれば、オリジナルコンテンツ１２１のハッシュ値を、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報１２３として生成する。

【００５４】また、たとえば、図形マークがロゴマークであり、そのロゴマークの真正さと、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ１２１との関係の真正さを認証可能とするのであれば、図形マーク１２３のハッシュ値と、オリジナルコンテンツ１２１のハッシュ値とを、それぞれ、その真正さを認める権威ある権威者や適当な第三者機関の秘密鍵で暗号化した電子署名を挿入情報１２３として生成する。

【００５５】または、これら以外の、認証可能とする真正さを認証するために必要な情報や、その他所望の情報、たとえば、日付情報などを含めた情報を挿入情報１２３として生成する。なお、サーバ側装置１００の利用者と、認証可能とする真正さを認める権威ある権威者や適当な第三者機関が異なる場合には、情報生成部１１３は権威者や適当な第三者機関の秘密鍵を知ることができないので、この場合は、入出力装置を介して権威者や適当な第三者機関側と情報をやりとりし、権威者や適当な第三者機関側に、権威者や適当な第三者機関の秘密鍵を用いた暗号化の依頼を、暗号化に必要な情報と共に送り、その応答として権威者や適当な第三者機関から送られた挿入情報を記憶部１２０に格納する。ここで、このような権威者や適当な第三者機関側と情報をやりとりは、もちろん、ネットワーク１０を介して行うようにしてよい。

【００５６】次に、情報挿入部１１４は、図形マーク１２３に、挿入情報１２２を埋め込む埋め込み処理を行う。

【００５７】図５に、この埋め込み処理の処理手順を示す。

【００５８】以下、その詳細を、図形マーク１２３が１２８×１２８画素の画像であり、各画素は、一つの輝度データと２つの色差データから構成され、挿入情報１２２が５５ビットの情報である場合を例にとり説明する。

【００５９】さて、埋め込み処理では、まず、挿入情報１２２を、各５ビットの７つのビット列と、２０ビットのビット列の８つのビット列に分割する。

【００６０】そして、まず、最初の５ビットのビット列を、サイズによる埋め込み（ステップ８０１）によって図形マーク１２３に埋め込む。このサイズによる埋め込みでは、図形マーク１２３の画像サイズを、縦横それぞれの画素数が、３２×ｎ＋ａになるように変更する。ここで、ａは、埋め込む５ビットのビット列が表す１０進数であり、ｎは、３２×ｎ＋ａを、最も図形マーク１２３の元の画像サイズ（この場合は１２８）に近くする数値である。

【００６１】なお、このような画像サイズの変更は、図形マーク１２３の拡大、縮小によって行ってもよいし、たとえば、変更後に画素値が増加するような場合には、特定色（たとえば白）の画素を付加することにより行ってもよい。

【００６２】このようにすることにより、図形マーク１２３の画像サイズは、５ビットの値によって、縦横それぞれについて１１５画素から１４６画素に変更することになる。したがって、このサイズによる埋め込みによる図形マーク１２３の画像サイズの変更の程度は、縦横それぞれについて１０数パーセント程度であるので、図形マーク１２３の視認性が大きく失われることはない。

【００６３】次に、次の５ビットのビット列を、輝度シフトによる埋め込み（ステップ８０２）によって図形マーク１２３に埋め込む。この輝度シフトによるよる埋め込みでは、図形マーク１２３の各輝度データを、その図形マーク１２３の全体の輝度データの平均値が３２×ｎ＋ａになるように変更する。ここで、ａは、埋め込む５ビットのビット列が表す１０進数であり、ｎは、３２×ｎ＋ａを、図形マーク１２３全体の元の輝度データの平均値に最も近くする数値である。

【００６４】次に、次の５ビットのビット列を、輝度コントラストによる埋め込み（ステップ８０３）によって図形マーク１２３に埋め込む。この輝度コントラストによるよる埋め込みでは、図形マーク１２３の各輝度データを、その図形マーク１２３の輝度コントラストが、３２×ｎ＋ａになるように変更する。ここで、ａは、埋め込む５ビットのビット列が表す１０進数であり、ｎは、３２×ｎ＋ａを、最も図形マーク１２３全体の元の輝度コントラストに近くする数値である。ここで、図形マーク１２３の全体の輝度コントラストは、図形マーク１２３全ての輝度データの標準偏差とする。

【００６５】以下、残りの二つの色差データについても、各々５ビットのビット列についての、色差シフトによる埋め込み（ステップ８０４、８０６）と、色差コントラストシフトによる埋め込み（ステップ８０５、８０７）を、輝度データと同様にして行う。

【００６６】そして、最後に、残った１０ビットを電子

透かしによって図形マーク１２３に埋め込み（ステップ８０８）、情報入り図形マーク１２４として記憶部１２０に格納する。

【００６７】ただし、以上のステップ８０１から８０７による情報の埋め込みは、全てを行う必要がない。埋め込みによる図形マークの視認性の劣化や、埋め込むべき情報のビット数に応じて、一部のみを実行したり、各ステップにおいて埋め込む情報のビット数を異ならせるようにする。また、輝度、色差表現の代わりにＲＧＢなどを画素値の表現用い、各色の平均値やコントラストとして情報を埋め込むようにしてもよい。

【００６８】また、ステップ８０８における電子透かしによる埋め込みを行う情報のビット数は、その埋め込みによって、輝度／色差の平均値や、輝度／色差コントラストのうち、情報の埋め込みに用いた値を整数にまるめた値を変化させない程度に押さえるようにする。

【００６９】以上のような処理によって、図形マークの視認性を保ちながら、従来の電子透かしのみによって情報を埋め込む場合に比べ、より多くのデータを埋め込むことが可能となる。

【００７０】さて、図２に戻り、マーク添付部１１５は、記憶部１２０に格納されたオリジナルコンテンツ１２１を編集し、情報入り図形マークを貼り付け、マーク添付コンテンツ１２５を作成し、記憶部１２０に格納する。オリジナルコンテンツ１２１への、情報入り図形マークを貼り付けは、具体的には、オリジナルコンテンツ１２１がHTML文書である場合には、HTML文書中に、情報入り図形マークファイルの場所（URL）を<IMG SRC>タグを用いて記述することにより行う。

【００７１】WWWサーバ部１１６は、Ｗｅｂページであるマーク添付コンテンツ１２５をネットワーク１０に公開する。

【００７２】以上、サーバ側装置１００が行う処理について説明した。

【００７３】以下、クライアント側装置２００の行う処理について説明する。

【００７４】ブラウザ部１３は、ネットワーク上のＷｅｂサーバよりＷｅｂページを取り込み、記憶部２２０に記憶すると共に、その内容を入出力部２１１よりユーザに出力する。

【００７５】情報入りマーク切り出し部２１４は、記憶部２２０に記憶されたＷｅｂページが、マーク添付コンテンツ１２５である場合に、入出力部２１１を介して認証処理を指示されると、マーク添付コンテンツ２２１より情報入り図形マーク２２２を切り出し、記憶部２２０に記憶する。情報抽出部２１５は、情報入り図形マーク２２２に埋め込まれた挿入情報２２３を復元し、記憶部２２０に記憶する。

【００７６】この情報抽出部２１５が行う挿入情報を復元する処理の手順を図６に示す。

【００７７】図示するように、この処理では、まず、情報入り図形マーク２２２の縦、横の画素数を求め、これを３２で割った値の余りを５ビットで表現した値を、５ビットの情報として復元する（ステップ９０１）。

【００７８】次に、情報入り図形マーク２２２全体の輝度データの平均値を求め、平均値を３２で割った値の余りを５ビットで表現した値を復元する（ステップ９０２）。

【００７９】そして、情報入り図形マーク２２２全体の輝度データのコントラストを求め、コントラスト値を３２で割った値の余りを５ビットで表現した値を復元する（ステップ９０３）。

【００８０】また、同様に、色差データ１、色差データ２についても、それぞれ、その平均値とコントラストより、５ビットづつ情報を復元する（ステップ９０４～９０７）。

【００８１】そして、最後に、情報入り図形マーク２２２に埋め込まれた電子透かしを従来と同様にして抽出し、これより１０ビットを復元する（ステップ９０１）。

【００８２】そして、以上で求めた各ビットを連結し、４５ビットの情報を復元し、処理を終了する。

【００８３】さて、図３に戻り、認証部２１６は、挿入情報２２３が認証可能としている事項の認証を行う。

【００８４】たとえば、図形マークがロゴマークであり、そのロゴマークの真正さを認証するのであれば、認証部２１６は、オリジナル図形マーク２２５のハッシュ値を求め、これと、挿入情報２２３を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報２２４で復号した値と比較し、一致した場合に、真正さを認証する。ここで、オリジナル図形マーク２２５は、このＷｅｂページを公開したサーバ側装置１００が正当なものであれば、サーバ側装置１００の図形マーク１２３と同じものであり、情報が埋め込まれる前の情報入り図形マーク２２２に相当する。

【００８５】ここで、オリジナル図形マーク２２５と公開鍵情報２２４は、別途、真正さを認める権威ある権威者や適当な第三者機関より別途信頼できる方法でブラウザ部２１３または入出力部２１１を介して入手し記憶部２２０に記憶する。

【００８６】また、たとえば、図形マークがロゴマークであり、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ１２１との関係の真正さするのであれば、マーク添付コンテンツ２２１から、情報入り図例マーク２２２を除いたオリジナルコンテンツを復元し、そのハッシュ値を求め、これと、挿入情報２２３を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報２２４で復号した値と比較し、一致した場合に、真正さを認証する。

【００８７】また、たとえば、図形マークがロゴマーク

であり、そのロゴマークの真正さと、そのロゴマークと、そのロゴマークが貼り付けられたオリジナルコンテンツ１２１との関係の真正さを認証可能とするのであれば、オリジナル図形マーク２２５のハッシュ値と、マーク添付コンテンツ２２１から、情報入り図例マーク２２２を除いたオリジナルコンテンツのハッシュ値とを求め、これと、挿入情報２２３を真正さを認める権威ある権威者や適当な第三者機関の公開鍵情報２２４で復号した値と比較し、一致した場合に、真正さを認証する。

【００８８】そして、認証部２１６は、認証した結果を入出力部２１１を介してユーザに通知する。

【００８９】ところで、以上のような認証処理は、ネットワーク１０上に信頼できる認証装置を設け、クライアント側装置２００の認証部２１６が、この認証装置と協調して行うようにしてもよい。

【００９０】たとえば、予め、認証装置に、オリジナルコンテンツやオリジナル図形マークや権威者や適当な第三者機関の公開鍵情報のうちのいずれかもしくは全てを登録しておくようにする。そして、認証時には、クライアント側装置２００の認証部２１６が挿入情報や、その他の認証処理に必要な情報をを認証装置にネットワーク１０介してを送り、認証装置が前述したような認証処理を行い、その結果をクライアント側装置２００の認証部２１６に返すようにする。

【００９１】なお、本実施形態に係るクライアント側装置２００の、情報入りマーク切り出し部２１４、情報抽出部２１５、認証部２１６は、ブラウザプログラムにより実現されるブラウザ部２１３に対するブラグインソフトウエアによって実現するようにしてもよい。また、この場合は、ブラウザ部２１３が行うマーク添付コンテンツの表示上で、情報入り図形マークがユーザによって選択されたときに、情報入りマーク切り出し部２１４、情報抽出部２１５、認証部２１６を実現するブラグインソフトウエアを起動し、前述した情報入りマーク切り出し部２１４、情報抽出部２１５、認証部２１６に選択された情報入り図形マークについての前述した処理を行わせるようにするのがよい。ただし、この場合には、情報入り図形マークのデータファイルには特別な拡張子などを与えることなどにより、ブラウザ部２１３が、この情報入り図形マークが、このようなブラグインソフトウエアによって処理されるべきものであることを認識できるようにする。

【００９２】また、本実施形態に係るサーバ側装置１００に、オリジナルコンテンツ１２１を生成、編集するエディタプログラムの実行によって実現されるエディタ部を備えるようにしてもよい。そして、この場合、前述した情報生成部１１３、情報挿入部１１４、マーク貼付部１１５は、エディタプログラムから利用可能なブラグインソフトウエアとして実現するようにしてもよい。この場合、このブラグインソフトウエアは、エディタプログラムが提供するメニューの選択によって、起動され、前述の情報生成部１１３、情報挿入部１１４、マーク貼付部１１５の処理を実行することによって、エディタプログラムが編集しているオリジナルコンテンツ１２１を編集してマーク添付コンテンツ１２５を生成する。

【００９３】以上、第１の実施形態について説明した。

【００９４】以下、第２の実施形態について説明する。

【００９５】本第２実施形態は、第１実施形態と、サーバ側装置１００の情報挿入部１１４の行う、挿入情報１２２の図形マーク１２３への埋め込み方と、クライアント側装置２００の情報入りマーク切り出し部２１４が行う切り出しと、情報抽出部２１５が行う挿入情報の抽出の仕方が異なる。

【００９６】第２実施形態における、情報挿入部１１４が行う挿入情報１２２について説明する。

【００９７】図７に示すように、本第２実施形態では、図形マーク１２３に第２の画像を添付する。

【００９８】第２の画像１２３０は、図８に示すように、たとえば、１２８×４０画素の画像であり、４×４画素ごとに３２０のブロックに分割されている。情報挿入部１１４は、たとえば、３００ビットの挿入情報１２２の各ビットを、３２０のブロック中の所定の規則に従った優先順序で選択した３００ブロックの各々に割当て、各ブロックをそのブロックに割り当てたビットの値に応じた色で塗りつぶす。たとえば、値１のビットを割り当てたブロックは黒で塗りつぶし、値０のビットを割り当てたブロックは白で塗りつぶす。そして、図形マーク１２３と第２の画像１２３０を、情報入り図形マーク１２４として記憶部１２０に格納する。

【００９９】なお、以上の処理におけるブロックは１×１画素のブロック、すなわち、画素そのものとしてもよく、この場合は、第２の画像のサイズはより小さくて済む。

【０１００】さて、この場合、マーク添付部１１５は、記憶部１２０に格納されたオリジナルコンテンツ１２１を編集し、情報入り図形マーク１２４として記憶部１２０に格納された、図形マーク１２３と第２の画像１２３０をオリジナルコンテンツ１２１に貼り付けて、マーク添付コンテンツ１２５を作成し、記憶部１２０に格納する。WWWサーバ部１１６は、Ｗｅｂページであるマーク添付コンテンツ１２５をネットワーク１０に公開する。

【０１０１】一方、クライアント側装置３００の、報入りマーク切り出し部２１４は、ユーザから認証処理を指示されると、前述した第２の画像を切り出し、記憶部２２０に記憶する。クライアント側装置３００の情報抽出部２１５は、所定の規則に従った優先順序で、第２の画像の３２０のブロック中の３００ブロックを選択し、各ブロックの塗りつぶし色をビット値に変換する。たとえば、白で塗りつぶされたビットは値０のビットに、黒で

塗りつぶされたビットは値１のビットに変換する。そして、変換したビットを連結し、３００ビットの挿入情報２２３を復元する。

【０１０２】次に、第３の実施形態について説明する。

【０１０３】本第３実施形態は、第１実施形態と、サーバ側装置１００の情報挿入部１１４の行う、挿入情報１２２の図形マーク１２３への埋め込み方と、クライアント側装置２００の情報抽出部２１５が行う挿入情報の抽出の仕方が異なる。

【０１０４】第３実施形態における、情報挿入部１１４が行う挿入情報１２２について説明する。

【０１０５】図９に示すように、本第２実施形態では、図形マーク１２３の背景部１２３２を、挿入情報１２２を埋め込んだ画像で置き換える。ここで、図形マーク１２３の背景部１２３２とは、図形マーク１２３中で有意な図形、文字１２３１を含んでいない部分を指す。図形マーク１２３の背景部の領域を判別する方法としてはさまざまな手法があるが、たとえば、予め、背景部の領域の画素値を特定の値として図形マーク１２３を作成したり、予め背景部の領域を示す情報（マスクレイヤや、αチャネルと呼ばれる情報など）を付加して図形マーク１２３を作成して、これら情報より背景部の領域を判別したりする手法などを用いることができる。

【０１０６】さて、情報挿入部１１４は、このようにして背景部の領域を判別したならば、その領域に含まれる、画素または所定サイズ（たとえば２×２画素）のブロックを、所定の規則に従って順次選択し、挿入情報１２２の各ビットを、選択した画素またはブロックの各々に順次割当て、各画素またはブロックを割り当てたビットの値に応じた色で塗りつぶす。たとえば、値１のビットを割り当てた画素またはブロックは黒で塗りつぶし、値０のビットを割り当てたブロックは白で塗りつぶす。そして、図形マーク１２３を、情報入り図形マーク１２４として記憶部１２０に格納する。

【０１０７】ただし、情報挿入部１１４は、このように挿入情報１２２のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるよう、この領域を示す情報（マスクレイヤや、αチャネルと呼ばれる情報など）を付加して図形マーク１２３を作成するようにしてもよい。

【０１０８】また、情報挿入部１１４は、このように挿入情報１２２のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるよう、挿入情報１２２のビットの値に応じて塗りつぶした画素またはブロックの領域の範囲を示す特定の画像パターンを図形マークに含めるようにしてもよい。たとえば、背景部の領域の画素またはブロックをラスタ順に走査した場合に、連続して走査されることになる画素またはブロックの領域の始まりと終わりの部分を特定のパターンで塗りつぶし、特定のパターンで塗りつぶした部分の間の背景部の領域の画素またはブロックを挿入情報１２２のビットの値に応じた色で塗りつぶすようにする。

【０１０９】また、挿入情報１２２のビットの値に応じて塗りつぶす色を、情報入り図形マーク１２３のビットの値に応じて塗りつぶした画素以外の画素で使用されていない色とすることにより、挿入情報１２２のビットの値に応じて塗りつぶした画素またはブロックの領域を識別できるようにしてもよい。これは、たとえば、塗りつぶす色を白と黒とするならば、塗りつぶした画素以外の白または黒の画素の色を幾分変更（たとえば、白は白に近い灰色に、黒は黒に近い灰色）することにより実現することができる。

【０１１０】一方、クライアント側装置３００の情報抽出部２１５は、まず、情報入り図形マーク２２２の背景部を前述した領域を示す情報や特定の画像パターンより識別し、その領域に含まれる、画素または所定サイズ（たとえば２×２画素）のブロックを、所定の規則に従って順次選択し、各画素またはブロックの塗りつぶし色をビット値に変換する。たとえば、白で塗りつぶされたビットは値０のビットに、黒で塗りつぶされたビットは値１のビットに変換する。そして、変換したビットを連結し、挿入情報２２３を復元する。

【０１１１】以上、本発明の実施形態について説明した。

【０１１２】

【発明の効果】以上のように、本発明によれば、イメージデータが表す画像の視認性をある程度保ちながら、イメージデータに情報を添付する新たな手法を提供することができる。

【０１１３】また、本発明は、Ｗｅｂページ上のロゴマークなどの小さい画像サイズのイメージデータにイメージデータが表す画像の視認性をある程度保ちながら添付した情報によって、そのイメージデータに関連する事項の真正さを認証可能とすることができる。

【図面の簡単な説明】

【図１】本発明の実施形態に係るＷＷＷシステムの構成を示すブロック図である。

【図２】本発明の実施形態に係るサーバ側装置の構成を示すブロック図である。

【図３】本発明の実施形態に係るクライアント側装置の構成を示すブロック図である。

【図４】一般的な電子計算機の構成を示すブロック図である。

【図５】本発明の第１実施形態において行う、図形マークへ情報を埋め込む処理の手順を示すフローチャートである。

【図６】本発明の第１実施形態に係る、情報が埋め込まれた図形マークから情報を抽出する処理の手順を示すフローチャートである。

【図７】本発明の第２実施形態に係る図形マークへの情

報の添付のようすを示す図である。

【図８】本発明の第２実施形態に係る、情報を埋め込んだ画像を示す図である。

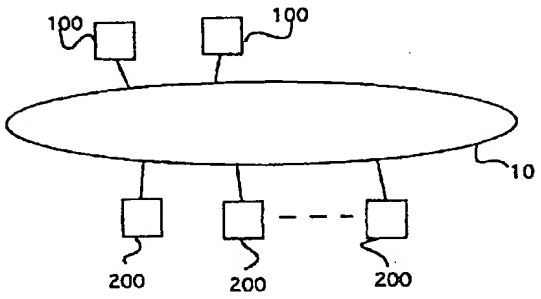
【図９】本発明の第３実施形態に係る、情報を埋め込んだ画像を示す図である。

【符号の説明】

１０　ネットワーク
１００　サーバ側装置
１１０　処理部
１１１　入出力部
１１２　サーバ側装置
１１３　情報生成部
１１４　情報挿入部
１１５　マーク貼付部
１１６　Ｗｅｂサーバ部
１２０　記憶部
２００　クライアント側装置
２１０　処理部
２２０　記憶部
２１１　入出力部
２１２　制御部
２１３　ブラウザ部
２１４　情報入りマーク切り出し部
２１５　報抽出部
２１６　認証部
２２０　記憶部

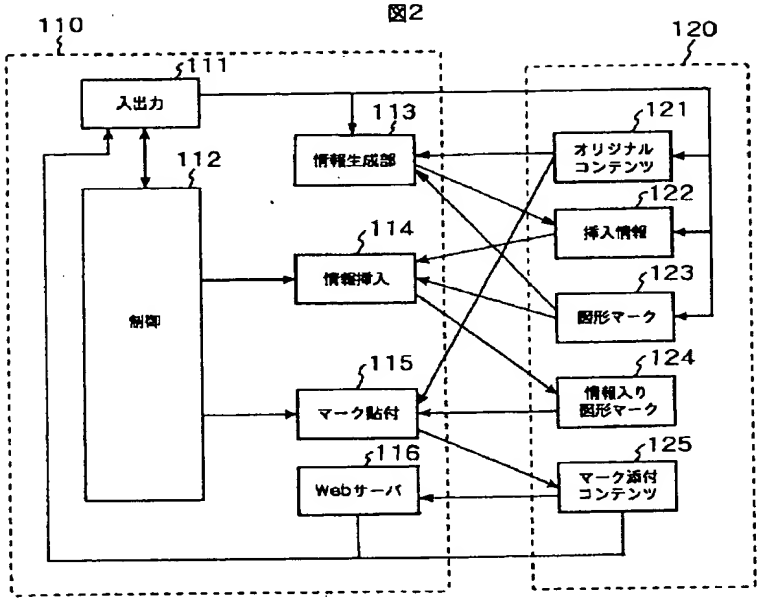
【図１】

図１



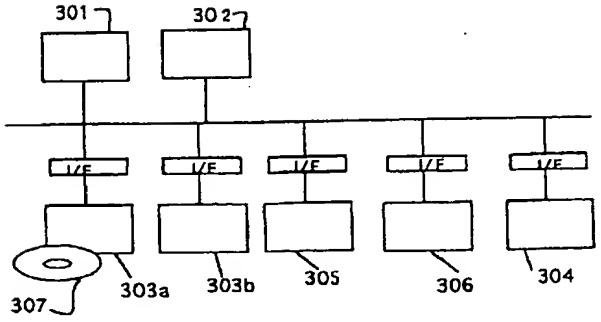
【図２】

図2



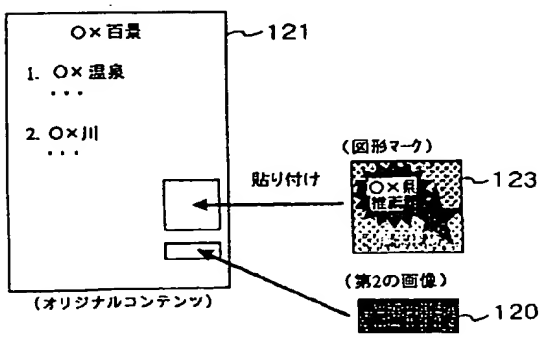
【図４】

図4



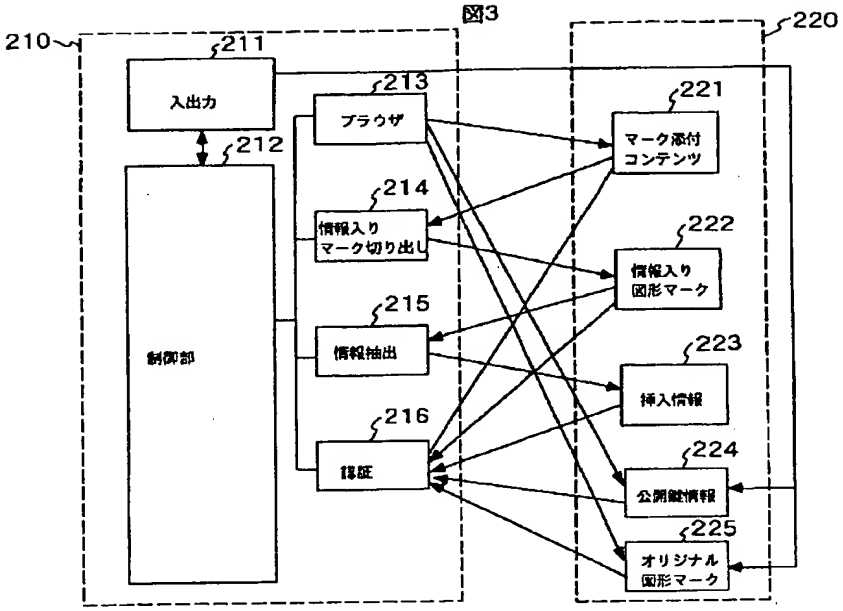
【図７】

図7



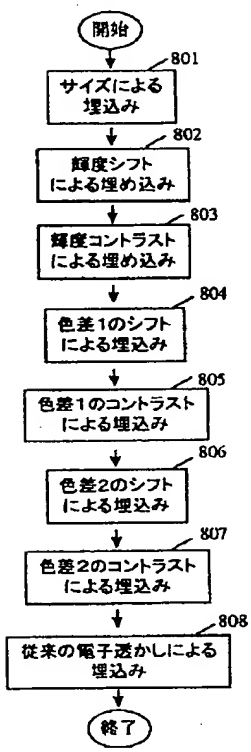
【図３】

図3



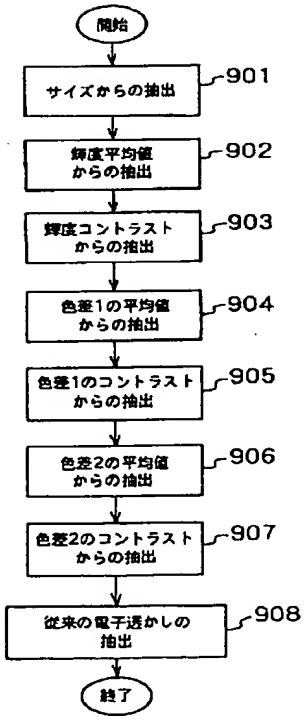
【図５】

図5



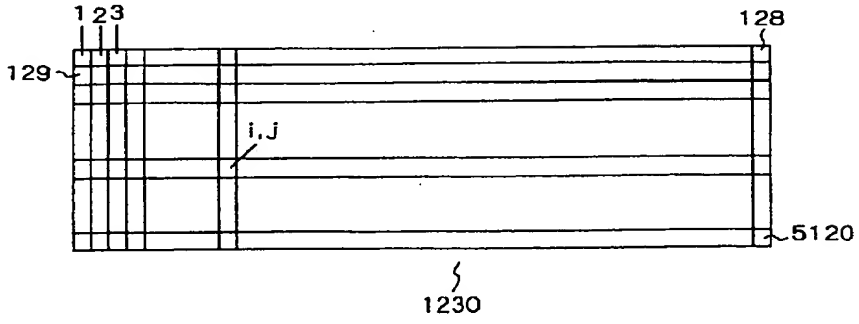
【図６】

図6



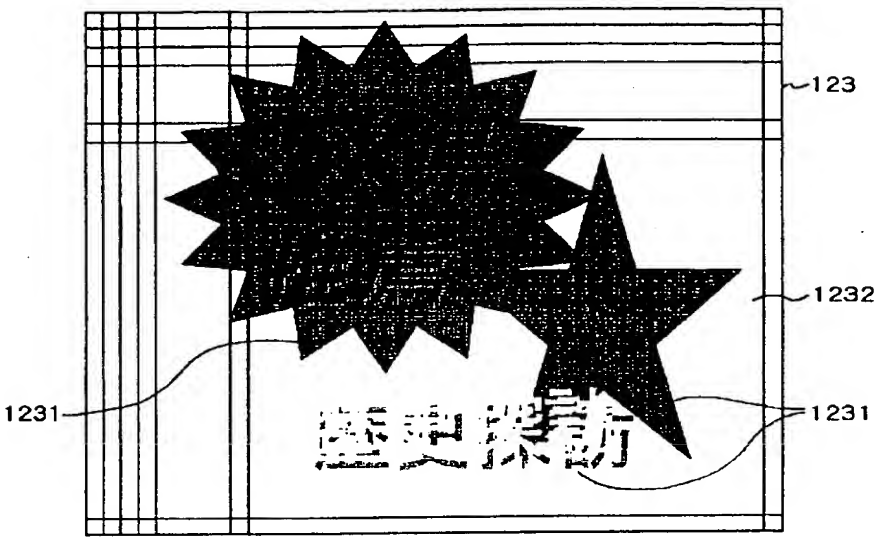
【図８】

図8



【図９】

図9



フロントページの続き

(72)発明者　永井　康彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　篠田　隆志
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内

Ｆターム(参考)　5B057 AA20 CA01 CA02 CA08 CA12
CA16 CB01 CB02 CB08 CB12
CB16 CC03 CD05 CE08 CE09
CE11 CE17 CG07 CG09 CH01
CH11 DA08 DA17 DB02 DB05
DB06 DB09 DC02
5C076 AA02 AA13 AA14 AA16 AA21
AA22 AA40 BA06 CA10 CB02